# *From the Editor*

Throughout history, states and militaries have sought to protect friendly information and information systems while attempting to attack and degrade their adversaries'. Today, during times of conflict, these efforts involve an integrated effort among intelligence cells, destructive systems, psychological and deception operations and electronic warfare.

As military analysts evaluate the relative strengths and weaknesses of America's Armed Forces and those of potential foes, the prevailing view is that the US military will not be challenged directly on a battlefield where our superior land, air and naval power can be brought to bear. Rather, challenges will be mounted indirectly on our information systems, what we call asymmetric attacks. For example, the specter of a computer network attack threatens US forces, and the entire nation, with everything from disruption to defeat.

This issue of *Military Review* picks up the thread of emerging threats where the last issue left off. While the July-August issue looked at regional threats to peace, this edition examines technologically derived threats that will disrupt not only the peace but the foundation of society as well. Moreover, the authors argue that these threats do not merely loom over the horizon, we face some of them now.

In the lead article, Flynt contends that in addition to well-known and exhaustively dissected challenges, America faces new and unprecedented threats—from hacker intrusions to biological attacks to the potential debacle of Y2K—that converge in targeting the US population and critical infrastructure.

Next, Murray looks at China's deception and perception-management programs, while Thomas examines China's knowledge warfare concepts and Russia's development of information-psychological operations and human behavior control mechanisms.

Clemmons and Brown explore three aspects of cyberwar: Are these techniques actually weapons? Are individuals who wage cyberwar combatants? And, are cyberwar's means weapons of mass destruction?

In his second article in this issue, Thomas ponders whether technology, by providing overwhelming amounts of information instantly, pushes fallible humans beyond their ability to process data and make wise judgments.

Bunker postulates that qualitative advances in civilization call for a redefinition of the military arts and sciences. He argues that "higher-dimensional" warfighting will require a fundamental shift in how the Army conducts future operations.

Shin, looking at the impact of a paradigmatic shift in civilization and how it will influence the nature of war, questions whether Force XXI will be relevant under fundamentally changed conditions.

Finally, Prinslow, Turbiville and Waller profile the Open-Source Information System, a private virtual network—an Intranet—that provides US government personnel access to foreign open-source material from which much can be learned about nations' capabilities and intentions.

***LJH***